UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER II
FINAL EXAMINATION SEMESTER II
SESI 2021/2022
SESSION 2021/2022
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD MATAPELAJARAN ***SUBJECT CODE***	**: BITS 3613**
MATAPELAJARAN ***SUBJECT***	**:TEKNIK PENGGODAMAN DAN PENCEGAHAN** ***HACKING TECHNIQUES AND PREVENTION***
PENYELARAS ***COORDINATOR***	**: MOHD ZAKI MAS'UD**
KURSUS ***COURSE***	**: 3 BITZ**
MASA ***TIME***	**: 2:15 Ptg to 4:15 Ptg** **2:15 P.M to 4:15 P.M**
TEMPOH ***DURATION***	**: 2 JAM** ***2 HOURS***
TARIKH ***DATE***	**: 25 JUN 2022** ***25 JUNE 2022***
TEMPAT ***VENUE***	**:**

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **Kertas soalan ini mengandungi DUA (2) Bahagian. Sila Jawab SEMUA soalan di kedua-dua Bahagian**
   The exam paper consists of TWO (2) PARTS. Please ALL the questions in both part
2. **Kertas soalan ini mempunyai versi dwi-bahasa.**
   The exam paper consists of dual-language version.

KERTAS SOALAN INI TERDIRI DARIPADA TUJUH (18) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS SEVEN (18) PAGES INCLUSIVE OF FRONT PAGE

BAHAGIAN A: SOALAN BERSTRUKTUR (40 MARKAH)

ARAHAN: *Sila jawab **SEMUA** soalan*

(a) Teknologi Internet telah berkembang secara drastik dalam beberapa tahun kebelakangan ini dan sekarang ini lebih banyak peranti telah disambungkan ke internet menyebabkan lebih banyak peranti terdedah kepada ancaman siber. Senaraikan apakah ancaman yang boleh dicetuskan oleh seorang penggodam terhadap sesebuah organisasi.

(4 markah)

(b) Penggodam boleh dikategorikan kepada beberapa jenis, senaraikan **EMPAT (4)** jenis penggodam.

(4 Markah)

(c) Berikan definisi kepada terma-terma penggodaman di bawah:-

i. *Zero Day Attack*

(1 mark)

ii. *Daisy Chaining*

(1 mark)

iii. *Exploit*

(1 mark)

iv. *Vulnerability*

(1 mark)

(d) Etika bermaksud piawai perbuatan yang salah dan betul manakala Undang-undang ditakrifkan sebagai peraturan kepada kelakuan atau tindakan yang dikuatkasakan secara rasmi oleh pihak berkuasa yang mempunyai bidang kuasa terhadap mereka. Nyatakan **EMPAT (4)** lagi perbezaan antara Etika dan Undang-undang.

(4 markah)

(e) Nyatakan **EMPAT (4)** undang-undang siber di Malaysia yang telah diluluskan oleh Parlimen Malaysia bagi melindungi rakyat dari jenayah siber.

(4 markah)

(f) Agen Smith telah berjaya memintas komunikasi di antara tentera Soviet dalam Perang Dunia ke I dan beliau percaya, mereka menggunakan kaedah *Caesar Cipher* untuk menyulitkan mesej mereka. Sebagai *cryptanalyst* kepada Agen Smith, cari kunci dan nyahsulit teks sifer berikut.

```
DROA ESOD OBIY ELOM YWOD ROWY BOIY EKBO KLVO DYROKB
```

(5 markah)

(g) Bincangkan mana-mana **LIMA (5)** Fasa penggodaman dalam mengeksploitasi kelemahan pada pelayan web.

(5 markah)

(h) Senaraikan **TIGA (3)** teknik yang digunakan dalam menyerang kata laluan.

(3 markah)

(i) Setelah fasa *foot printing* dan *enumeration* selesai, fasa seterusnya dalam proses penggodaman ialah penggodaman sistem dan ia terdiri daripada lima peringkat. Senaraikan mana-mana **TIGA (3)** daripada peringkat penggodaman sistem.

(3 markah)

(j) Ujian Penerobosan boleh dilaksanakan sama ada melalui pendekatan dari dalam organisai atau luar organisasi. Terangkan setiap pendekatan tersebut serta senaraikan kelebihan dan kekurangan untuk setiap satu pendekatan.

(4 markah)

BAHAGIAN B: SOALAN BERSTRUKTUR (60 MARKAH)

ARAHAN: *Sila jawab **SEMUA** soalan*

SOALAN 1 (20 MARKAH)

Kajian Kes 1:

Jamian97 adalah seorang penggodam *blackhat* yang telah berjaya mengeksploitasi dan menembusi komputer pelayan milik syarikat Darsani Corporation Berhad (DCB). Sebagai Pengurus Kanan Keselamatan Komputer DCB, anda telah diminta untuk melakukan siasatan ke atas kejadian tersebut. Berdasarkan penyiasatan pada log rangkaian yang ditangkap dari komputer pelayan seperti di lampiran **Appendix 1**, pencerobohan keselamatan dilakukan menggunakan metodologi penggodaman yang piawai. Bincangkan penyiasatan anda tentang insiden tersebut berdasarkan metodologi penggodaman untuk dijelaskan kepada pengurusan atasan,

Untuk membantu penyiasatan anda, jawab soalan berikut berdasarkan metodologi penggodaman:

(a) Kejuruteraan Sosial adalah salah satu kaedah yang licik untuk memanipulasi kecenderungan semulajadi manusia untuk mempercayai seseorang dan merupakan salah satu pendekatan untuk mengumpulkan maklumat dari sasaran. Terangkan secara ringkas kaedah kejuruteraan sosial berikut. Bagi setiap kaedah tersebut, berikan contoh tindakan yang boleh dilakukan.

i. *Baiting* (2M)
ii. *Pretext* (2M)
iii. *Quod for quo* (2M)

(b) Cari komunikasi yg disyaki berlaku antara mesin Jamian97 dengan salah satu pelayan DCB dalam log trafik rangkaian ***Appendix 1***.

Berdasarkan log trafik rangkaian di ***Appendix 1***:

i. Kenalpasti alamat IP penggodam. (1 M)
ii. Apakah kaedah *port scanning* yang digunakan? Nyatakan alasan anda. (2 M)
iii. Kenalpasti **DUA (2)** port yang terbuka dan **DUA (2)** port yg tertutup semasa aktiviti *scanning* ini. (4 M)

iv. Berikan **DUA (2)** jenis perkhidmatan yang mungkin sedang berfungsi dalam pelayan tersebut. (2M)

v. Berdasarkan aktiviti *scanning* tersebut ada beberapa port yang terbuka, cadangkan **DUA (2)** langkah pengukuhan yang boleh dilakukan oleh pengurus keselamatan dalam memperkukuhkan keselamatan pelayan tersebut. (2M)

(c) Dari maklumat yang dijumpai dalam soalan b, cadangkan **TIGA (3)** jenis serangan yang mungkin dilakukan terhadap pelayan DCB. (3M)

(20 markah)

SOALAN 2 (20 MARKAH)

Kajian Kes 2:

GreenWill Sdn. Bhd. ialah sebuah syarikat perisian yang terkenal dan berkepakaran dalam membangunkan aplikasi web. Antara tatacara piawai syarikat ini adalah menganalisis setiap kod yang dibangunkan oleh pengaturcara untuk memastikan ia ditulis dengan selamat dan melakukan penilaian tahap keselamatan pelayan wab yang menempatkan sistem. Sebagai pengaturcara kanan anda perlu menyediakan kriteria amalan pembangunan sistem dalam talian yang selamat serta ciri-ciri konfigurasi pelayan web yang selamat kepada pengaturcara junior. Bincangkan dengan terperinci kriteria pembangunan perisian selamat dan konfigurasi pelayan web selamat dalam memastikan keselamatan sistem aplikasi atas talian.

Untuk membantu membincangkan keselamatan sistem aplikasi dalam talian, jawab soalan berikut berdasarkan amalan piawai syarikat tentang menganalisis pembangunan kod dan konfigurasi pelayan web yang selamat.

(a) Cadangkan **EMPAT (4)** kesilapan konfigurasi yang mungkin berlaku kepada pelayan web yang boleh menyebabkan aplikasi web diserang oleh penggodam. (4M)

(b) Kenalpasti **EMPAT (4)** impak apabila pelayan web mempunyai kelemahan. (4M)

(c) Senaraikan **DUA (2)** kaedah serangan yang boleh dilakukan kepada pelayan web tersebut. (2M)

(d) Tentukan nama bagi setiap serangan aplikasi web dibawah dan berikan **SATU (1)** kaedah untuk mencegah serangan untuk senario tersebut berdasarkan senarai kelemahan aplikasi web OWASP.

i. Zamri telah log masuk ke aplikasi dalam talian pada komputer awam dan hanya menutup pelayar web tanpa log keluar dengan betul dari aplikasi dalam talian. Selepas sejam seorang penggodam menggunakan komputer yang sama dan boleh mengakses akaun pengguna Zamri dengan hanya membuka pelayar web yang sama. (2M)

ii. Penyerang memantau trafik rangkaian antara komputer Eliza dan domain perbankan dalam talian dan kemudian menurunkan taraf sambungan daripada HTTPS kepada HTTP, yang membolehkan penyerang memintas permintaan dan mencuri kuki sesi pengguna. Penyerang kemudian memainkan semula sesi kuki ini menyebabkan penyerang boleh merampas sesi pengguna (disahkan), mengakses atau mengubah suai data peribadi pengguna. (2M)

iii. Dengan menggunakan pelayar web Robert melawat *http://www.myua.edu.my/web* dan menemui senarai nama fail yang disenaraikan pada pelayar web, tiga daripada fail tersebut merupakan fail kelas java terkumpul yang boleh dimuat turun. Robert yang merupakan seorang pemburu kod terlatih berjaya menyahkompilasi dan merekayasa balik fail kelas java tersebut. Melalui analisis yang dilakukan terhadap fail itu, Robert telah menemui beberapa kelemahan pada sistem tersebut. (2M)

iv. Penyerang hanya mengubah parameter 'acct' dalam ruangan URL pelayan web yang memaparkan http://example.com/app/accountInfo?acct=129834568129 dengan beberapa nombor rawak 12 digit dan berjaya mengakses akaun pengguna lain. (2M)

(e) Semasa sesi demonstrasi serangan aplikasi web, log pelayan web telah menangkap beberapa aktiviti yang luar biasa yang dilakukan terhadap pelayan web. Rajah 1 menunjukkan log pelayan web tersebut.

```
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit
=Submit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit
=Submit" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:58 -0400] "GET
/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd
HTTP/1.1" 200 5717 "-" "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:23:21 -0400] "GET
/dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4333
"http://192.168.254.133/dvwa/vulnerabilities/fi/?page=../../..
/../../etc/passwd" "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36"
```

Rajah 1: log pelayan web

Berdasarkan Rajah 1,

i. Daripada log pelayan web, Namakan jenis serangan aplikasi web yang telah dilaksanakan oleh penyerang. (1M)

ii. Cadangkan **SATU (1)** mekanisma pertahanan yang boleh digunakan untuk mencegah serangan begini. (1M)

(20 markah)

SOALAN 3 (25 MARKAH)

Kajian Kes 3:

PT Cepat Sdn. Bhd. (PTCSB) telah diberikan tanggungjawab oleh Aliman Resources Sdn. Bhd. (ARSB) untuk melaksanakan ujian penembusan terhadap infrastruktur dan infostruktur ICT. Sebagai penguji penembusan kanan dalam PTCSB, anda perlu mencadangkan skop ujian penembusan kepada Ketua Pegawai Maklumat ARSB, bincangkan secara terperinci ujian tersebut berdasarkan metodologi ujian penembusan.

Perbincangan anda perlu merangkumi perkara-perkara berikut:

(a) **TIGA (3)** kategori penilaian keselamatan. (3M)

(b) **TIGA (3)** sebab kenapa Pengujian Penembusan perlu dilakukan ke atas infrastrukutur ICT ARSB. (3M)

(c) **EMPAT (4)** ruang lingkup ujian penembusan yang perlu dilakukan untuk menjamin keselamatan infrastruktur dan infostruktur ICT di syarikat ARSB. (4M)

(d) **DUA (2)** teknik yang boleh digunakan dalam mengesan SSID tanpa wayar. (2M)

(e) **EMPAT (4)** langkah yang mungkin dilakukan oleh pasukan PTCSB dalam menembusi AP tanpa wayar yang dipercayai dikonfigurasikan dengan pengesahan WPA. (4M)

(f) **EMPAT (4)** langkah yang boleh dicadangkan kepada ARSB dalam mencegah serangan terhadap rangkaian tanpa wayar pada masa akan datang. (4M)

(20 markah)

-SOALAN TAMAT-

PART A: STRUCTURED QUESTIONS (40 MARKS)

INSTRUCTION: *Answer **ALL** questions.*

(a) Internet Technology has evolved drastically in recent years and nowadays more devices are connected to the internet, thus exposing more devices to cyber threat. List **FOUR (4)** threats a hacker can cause to an organization.

(4 marks)

(b) Hackers nowadays can be categorized into several types of hackers, list **FOUR (4)** different types of hackers.

(4 marks)

(c) Define the following hacking terminology: -

i. Zero Day Attack

(1 mark)

ii. Daisy Chaining

(1 mark)

iii. Exploit

(1 mark)

iv. Vulnerability

(1 mark)

(d) Ethic is defined as the standard of right and wrong, whereas Law is defined as a set of rules on conduct or action prescribed or formally recognized as binding or enforced by a controlling authority. State another **FOUR (4)** differences between ethics and law.

(4 marks)

(e) State **FOUR (4)** Malaysian Cyberlaw that have been passed by Malaysia's parliament in protecting the citizen from cyber related crime.

(4 marks)

(f) Agent Smith has successfully intercepted a communication between the Soviet army in the World War I and believed to be using Caesar cipher to encrypt their message. As a cryptanalyst for Agent Smith, decrypt and find the key for the ciphertext.

DROA ESOD OBIY ELOM YWOD ROWY BOIY EKBO KLVO DYROKB

(5 marks)

(g) Discuss any **FIVE (5)** hacking phases in exploiting the vulnerabilities on web server.

(5 marks)

(h) List **THREE (3)** techniques used in attacking password.

(3 marks)

(i) Once foot printing and enumeration phase is complete, the next phase in a hacking process is system hacking and it consist of five stages. List any **THREE (3)** of the system hacking stages.

(3 marks)

(j) Penetration Testing can be performed either from the internal site or external site. Describe each of the approach and list the advantage and disadvantage of each of them.

(4 marks)

PART B: STRUCTURED QUESTIONS (60 MARKS)

INSTRUCTION: *Answer **ALL** questions.*

QUESTION 1 (20 MARKS)

Case Study 1:

Jamian97 is a black hat hacker who has successfully exploited and penetrated a server owned by Darsani Corporation Berhad (DCB). As the Computer Security Senior Manager of DCB you are asked to do an investigation on this security breach. Based on the investigation on the network log captured from the server as shown in **Appendix 1**, the security breach is done using standard hacking methodology. Discuss your investigation of the incident based on the hacking methodology to explain to the top management.

To guide your investigation, answer the following questions based on hacking methodology:

(a) Explain each of the social engineering method based on an example of an action plan to trace the hacking activities.

i. Baiting (2M)
ii. Pretext (2M)
iii. Quod for quo (2M)

(b) Find the suspected communication between Jamian97's machine and DCB's server from the network traffic log in **Appendix 1**.

i. The attacker's IP address. (1M)
ii. Type of port scanning method is used and state your reason. (2M)
iii. **TWO (2)** open and **TWO (2)** close ports during this scanning activity. (4M)
iv. **TWO (2)** type of services that might be running on the server. (2M)
v. Propose **TWO (2)** actions the security administrator can take to harden the server security based on the open port found in the scanning activity. (2M).

(c) Suggest **THREE (3)** types of attack that might be launched to attack the DCB's server based the finding in (b). (3M)

(20 marks)

QUESTION 2 (20 MARKS)

Case Study 2:

GreenWill Sdn. Bhd. is a software development company which is expert in developing online applications. Among the standard practice by the company before deploying an online system are analysing each code developed by the programmers to make sure it is written securely and evaluating the security level of web server that hosting the system. As a senior programmer you need to provide criteria of a secure online system development practice to the junior programmer as well as the characteristic of good web server configuration. Discuss in detail the criteria of a secure software development and a secure web server configuration in ensuring the security of an online application system.

To guide your discussion in ensuring the security of an online application system, answer the following questions based on company standard practices on analysing code development and secure web server configuration.

(a) Suggest **FOUR (4)** misconfigurations in a web server that can lead to web application attacked by hacker. (4M)

(b) **Identify FOUR (4)** impacts of a vulnerable webserver. (4M)

(c) **List** any **TWO (2)** of the attack methods to attack webserver. (2M)

(d) Determine the correct name of web application attack and give **ONE (1)** method to prevent the attack for the scenario based on OWASP top 10 web application vulnerabilities.

i) Zamri has login into an online application on a public computer and just closed the web browser without logging out properly from the online application. After an hour later a hacker uses the same computer and is able to access Zamri's user account by just opening the same web browser. (2M)

ii) An attacker monitors the network traffic between Eliza's computer and an online banking domain and then downgrades the connections from HTTPS to HTTP which enable the attacker to intercept requests and steal the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data. (2M)

iii) Using a web browser, Robert visited *http://www.myua.edu.my/web* and found a list of file names listed on the web browser, in which 3 of the files is recognized as a compiled java classes files that can be downloaded. Robert who is a trained code bounty hunter is able to decompile and reverse engineer the java classes file. Through the analysis Robert's found several flaws on the system. (2M)

iv) An attacker simply modifies the 'acct' parameter in the browser which displayed http://example.com/app/accountInfo?acct=129834568129 with some random 12 digits number and able to access a random user's account. (2M)

(e) During the demonstration session on web application attack, the webserver log had captured some unusual activity done towards the server. Figure 1 shows the webserver log

```
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit=Submit
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:50 -0400] "GET
/dvwa/vulnerabilities/fi/?page=include.php HTTP/1.1" 200 4083
"http://192.168.254.133/dvwa/vulnerabilities/sqli/?id=3&Submit=Submit
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:18:58 -0400] "GET
/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd HTTP/1.1"
200 5717 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
192.168.254.172 - - [09/Apr/2022:00:23:21 -0400] "GET
/dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4333
"http://192.168.254.133/dvwa/vulnerabilities/fi/?page=../../../../../
etc/passwd" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36"
```

Figure 1: web server log

Based on Figure 1,

i. Name the type of web application attack that has been executed by the attacker. (1M)

ii. Suggest **ONE (1)** defense mechanism that can be used to prevent this attack. (1M)

(20 marks)

QUESTION 3 (20 MARKS)

Case Study 3:

PT Cepat Sdn. Bhd. (PTCSB) is hired by Aliman Resources Sdn. Bhd. (ARSB) to perform a penetration testing to its ICT infrastructure and info structure. As a senior Pen Tester in PTCSB you need to propose the scope of penetration testing to the Chief Information Officer of ARSB, Discuss the proposal in detail based on the penetration testing methodology.

Your discussion must include the following:

(a) **THREE (3)** categories of Security Assessment. (3M)

(b) **THREE (3)** reasons why Penetration Testing need to be performed on ARSB ICT infrastructure. (3M)

(c) **FOUR (4)** scopes of penetration testing need to be done to secure the ARSB's ICT infrastructure and info structure . (4M)

(d) **TWO (2)** techniques that can detect the availibility of wireless SSID in the organization to start a penetration testing on a wireless network infrastructure. (2M)

(e) **FOUR (4)** steps the PTCSB team might apply in penetrating the wireless Access Point (AP), which is believed to be configured with WPA authentication and has the potential to be exploited because of the wireless AP vulnerability in the configuration setting. (4M)

(f) **FOUR (4)** recommended countermeasures that ARSB can apply to the wireless network for future attack prevention. (4M)

(20 marks)

-END OF QUESTION-

APPENDIX I

The network traffic captured during the hacking incidents in DCB

No.	Source	scport	Destination	Dt port	Prtcl	Info
1	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [SYN]
2	192.168.254.132	445	192.168.254.172	36436	TCP	microsoft-ds > 36436 [SYN, ACK]
3	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [SYN]
4	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [SYN]
5	192.168.254.132	80	192.168.254.172	42420	TCP	http > 42420 [SYN, ACK]
6	192.168.254.132	135	192.168.254.172	54766	TCP	epmap > 54766 [SYN, ACK]
7	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [SYN]
8	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [ACK]
9	192.168.254.132	139	192.168.254.172	42230	TCP	netbios-ssn > 42230 [SYN, ACK]
10	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [ACK]
11	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [ACK]
12	192.168.254.172	53720	192.168.254.132	25	TCP	53720 > smtp [SYN]
13	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [ACK]
14	192.168.254.132	25	192.168.254.172	53720	TCP	smtp > 53720 [RST, ACK]
15	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [SYN]
16	192.168.254.132	3306	192.168.254.172	38686	TCP	mysql > 38686 [SYN, ACK]
17	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [SYN]
18	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [ACK]
19	192.168.254.132	21	192.168.254.172	47218	TCP	ftp > 47218 [SYN, ACK]
20	192.168.254.172	46770	192.168.254.132	110	TCP	46770 > pop3 [SYN]
21	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [ACK]
22	192.168.254.132	110	192.168.254.172	46770	TCP	pop3 > 46770 [RST, ACK]
23	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [SYN]
24	192.168.254.132	443	192.168.254.172	43844	TCP	https > 43844 [SYN, ACK]
25	192.168.254.172	48756	192.168.254.132	22	TCP	48756 > ssh [SYN]
26	192.168.254.132	22	192.168.254.172	48756	TCP	ssh > 48756 [RST, ACK]
27	192.168.254.172	36436	192.168.254.132	445	TCP	36436 > microsoft-ds [RST, ACK]
28	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [ACK]
29	192.168.254.172	42420	192.168.254.132	80	TCP	42420 > http [RST, ACK]
30	192.168.254.172	54766	192.168.254.132	135	TCP	54766 > epmap [RST, ACK]

31	192.168.254.172	42230	192.168.254.132	139	TCP	42230 > netbios-ssn [RST, ACK]
32	192.168.254.172	38686	192.168.254.132	3306	TCP	38686 > mysql [RST, ACK]
33	192.168.254.172	47218	192.168.254.132	21	TCP	47218 > ftp [RST, ACK]
34	192.168.254.172	43844	192.168.254.132	443	TCP	43844 > https [RST, ACK]
35	192.168.254.172	42632	192.168.254.132	143	TCP	42632 > imap [SYN]
36	192.168.254.132	143	192.168.254.172	42632	TCP	imap > 42632 [RST, ACK]
37	192.168.254.172	39424	192.168.254.132	53	TCP	39424 > domain [SYN]
38	192.168.254.132	53	192.168.254.172	39424	TCP	domain > 39424 [RST, ACK]
39	192.168.254.172	33856	192.168.254.132	161	TCP	33856 > snmp [SYN]
40	192.168.254.132	161	192.168.254.172	33856	TCP	snmp > 33856 [RST, ACK]
41	192.168.254.172	42936	192.168.254.132	123	TCP	42936 > ntp [SYN]
42	192.168.254.132	123	192.168.254.172	42936	TCP	ntp > 42936 [RST, ACK]
43	192.168.254.172	50564	192.168.254.132	20	TCP	50564 > ftp-data [SYN]
44	192.168.254.132	20	192.168.254.172	50564	TCP	ftp-data > 50564 [RST, ACK]