UBND THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG LÝ TỰ TRỌNG THÀNH PHỐ HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐỀ THI KẾT THÚC HỌC PHẦN LÝ THUYẾT

HỌC KỲ: I **NĂM HỌC: 2019 – 2020**

Đề số 2

Bậc đào tạo: CAO ĐẲNG (C2)

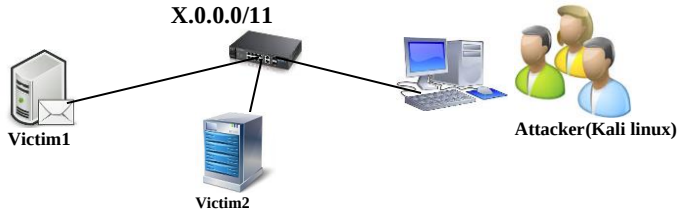
Học phần: KỸ THUẬT HACK

Lớp: 19C2-QTM Ngày thi: ____ / ____ / 2020

Thời gian thi: 90 phút *(không kể thời gian phát đề)*

(Thí sinh không được sử dụng tài liệu)

Cho mô hình mạng :



Câu 1: Tấn công nên tảng Android(victim1 là mạng trong nội bộ) theo sơ đồ mạng? *(4 điểm)*

- Chụp hình mình hoạ. Lưu tại D:\Hotensv\Cau1.pnp*

Câu 2: Tấn công khai thác lỗi HDH (victim2 là máy windows 7): Tắt/mở tường lửa, tạo user người dùng và nâng cấp lên quyền admin ? *(6 điểm)*

Lưu ý: Tất cả kết quả được lưu dươi dạng file *.png tại D:\Hoten_SV

_____Hết_____

GHI CHÚ: CÁN BỘ COI THI KHÔNG GIẢI THÍCH GÌ THÊM.

TRƯỞNG KHOA	TRƯỞNG BỘ MÔN	GIẢNG VIÊN RA ĐỀ
(Ký tên và ghi rõ họ tên)	*(Ký tên và ghi rõ họ tên)*	*(Ký và ghi rõ họ tên)*
NGUYỄN KHOA	***Nguyễn Văn Đôn***	***Dương Ngọc Vọng***

Họ tên sinh viên: *Số máy:*

UBND THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG LÝ TỰ TRỌNG THÀNH PHỐ HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐỀ THI KẾT THÚC HỌC PHẦN LÝ THUYẾT

HỌC KỲ: I **NĂM HỌC: 2019 – 2020**

Đề số 1

Bậc đào tạo: CAO ĐẲNG (C2)

Học phần: KỸ THUẬT HACK

Lớp: 19C2-QTM Ngày thi: ____ / ____ / 2020

Thời gian thi: 90 phút *(không kể thời gian phát đề)*

(Thí sinh không được sử dụng tài liệu)

– **Cho mô hình mạng sau:** *(cần có kết nối internet)*

Câu 1: [5 điểm] ***Hack với mã lỗi MS08-067*** -→Lấy Password gồm danh sách các user sau:
Administrators (Aministrator, admin, your_name)
Users(user1, user2, user2,hung, lan, minh)
P/S: Tất cả các user đều phải set password

Câu 2: [5 điểm] Sử dụng file từ điển (C:\passwd.txt) để lấy password của user thuộc group Administrators ? Sau đó tải công cụ psexec.exe để xâm nhập vào hệ thống và tạo một thư mục tại: ***C:\windows\system32\Hacked!*** --→Thực hiện vô hiệu hoá 1 user bất kỳ thuộc group Administrators -→tạo thêm user hacked với password là hacked!
Lưu ý: Tất cả kết quả được lưu dươi dạng file *.png tại D:\Hoten_SV

_____Hết_____

GHI CHÚ: CÁN BỘ COI THI KHÔNG GIẢI THÍCH GÌ THÊM.

TRƯỞNG KHOA	TRƯỞNG BỘ MÔN	GIẢNG VIÊN RA ĐỀ
(Ký và ghi rõ họ tên)	*(Ký và ghi rõ họ tên)*	*(Ký và ghi rõ họ tên)*
NGUYỄN KHOA	***Nguyễn Văn Đôn***	***Dương Ngọc Vọng***

Họ tên sinh viên: *Số máy:*

UBND THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG LÝ TỰ TRỌNG THÀNH PHỐ HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Đ c lập - Tự do - Hạnh phúc

ĐÁP ÁN ĐỀ THI KẾT THÚC HỌC PHẦN LÝ THUYẾT

HỌC KỲ: II NĂM HỌC: 2018 – 2019

Bậc đào tạo: CAO ĐẲNG(C1)

Học phần: KỸ THUẬT HACK NÂNG CAO

Lớp: 17C1-ANM Ngày thi: ____ / ____ / 2019

Thời gian thi: 90 phút *(không kể thời gian phát đề)*

Đề số 2

(Thí sinh không được sử dụng tài liệu)

Câu	Ý	Đáp án	Điểm
1		– Thiết lập IP theo sơ đồ mạng – Tạo Backdoor *.exe từ máy Attacker→Gởi mail cho máy nạn nhân – Từ máy Android truy cập gmail và tải backdoor – Thực thi backdoor – Lắng nghe port mở – Tiến hành khai thác – Chụp hình minh hoạ	0.5 đ 1.0 đ 0.5 đ 0.5 đ 0.5 đ 0.5 đ 0.25 đ 0.25 đ
2		✓ Sử dụng msfvenom tạo backdoor xxx.exe ✓ Chép backdoor vào đường dẫn /www/var/html/backdoor ✓ Khởi tạo dịch vụ apache2 ✓ Download tại đường dẫn http://ip_acttacker ✓ Chạy để thực thi backdoor xxx.exe ✓ Tiến hành khai thác lỗi và chụp hình minh hoạ ✓ Chụp hình minh chứng	1.0 đ 1.0 đ 1.0 đ 1.0 đ 1.0 đ 0.75 đ 0.25 đ

(Ký và ghi rõ họ tên) *(Ký và ghi rõ họ tên)*

Nguyễn Văn Đôn ***Dương Ngọc Vọng***

Họ tên sinh viên: *Số máy:*

UBND THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG CAO ĐẲNG LÝ TỰ TRỌNG THÀNH PHỐ HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐÁP ÁN ĐỀ THI KẾT THÚC HỌC PHẦN THỰC HÀNH

HỌC KỲ: II NĂM HỌC: 2018 – 2019

Bậc đào tạo: CAO ĐẲNG (C1)

Học phần: KỸ THUẬT HACK NÂNG CAO

Lớp: 17C1-ANM Ngày thi: ____ / ____ / 2019

Thời gian thi: 90 phút *(không kể thời gian phát đề)*

(Thí sinh không được sử dụng tài liệu)

Đề số 1

Câu	Ý	Đáp án	Điểm
1		– Thiết lập IP theo sơ đồ – Sử dụng msfconsole – Khai thác mã lỗi ms08_067_netapi – Set IP Lhost – Set IP Rhost – Khai thác lỗi – Tạo danh sách user – Add vào group admin – Chụp hình minh chứng	0.5 đ 0.5 đ 0.5 đ 0.5 đ 0.5 đ 0.5 đ 0.5 đ 0.25 đ 0.25 đ
2		– Tạo file từ điển chứa password dự đoán – Dùng vòng lặp For truy vấn password – Lấy password administrator – Dùng công cụ psexec.exe tấn công với passowrd đã được crack – Vô hiệu quá tài khoản guest – Tạo folder C:\windows\system32\hacked! – Chụp hình minh chứng.	1.0 đ 1.0 đ 1.0 đ 1.0 đ 1.0 đ 0.75 đ 0.25 đ

(Ký và ghi rõ họ tên) *(Ký và ghi rõ họ tên)*

Nguyễn Văn Đôn ***Dương Ngọc Vọng***

Họ tên sinh viên: *Số máy:*