Date: ۱۴۰۰/۹/۲۱ ۹۷۵۲۱۰۱۸ رامتین احسانی Subject: یادداشت کلاسی

* مسیریابی در روتر ← spanning tree Protocol ← STP

← مبتنی بر اصل راست گویی

← X Authentication X

* جلوگیری از loop ←

← هکرها می‌توانند اذیت کنند

← ایجاد حلقه loop

* exploit ← technique
payload ← ایجاد باگ

← divert exec path

* exploit ← وابسته به معماری باگ

* نیازمندی ها ← shell
connection

* چرا shellcode؟ ← برای پیدا کردن network

* ساختار shellcode؟ ← getting EIP
Decoder
get address
Socket
spawn shell

Date: / /   Subject:

* EIP ← جایی که CPU درحال اجرای کد است

← extended Instruction pointer

any Win32 ← GetProcAddress() ← get address *

* هدف ؟ ← وارد kernel32 بشیم ← وارد PE

← رسیدن به export table

STARTUPINFO ← Spawn *

launch cmd.exe ← CreateProcess() با ←

تا کاربر نتواند ببیند ← redirekt ← input/output/err

* Win32 API ← توی DLL های مختلف

← هرچیزی توی این پنجره داره اجرا می شود

* برای connection ← نیاز به سوکت ←

bind
listen
accept

Date: / /

Subject:

* اگر کاربر پشت فایروال باشد ← استفاده از : Reverse Connect

* Reverse ← { Startup
Socket
Connect

* مهمترین آسیب پذیری ← اشتباهات فردی ← بالای ۹۰%

* { Social engineering ← مهندسی اجتماعی

  حدس رمز عبور ← { دیکشنری

  Brute-force