SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

CMPT 479/980: Systems and Network Security

Spring 2020

Review

Instructor: Khaled Diab

Today…

- What did we learn?
- What is next?

Course Goals

- Learn how an attacker gains control of a system
- Learn how to defend a system
- Gain hands-on experience in various system security topics
- Technical aspects of security
  - Reproducing attacks
  - Building defensive solutions

Course Summary

- Concepts:
  - Question every assumption
  - Root of evil: Mixing code and data
  - Design principles
  - …

- 21 Attacks
- 9 Defenses
- Tools and Skills
  - gcc, gdb, ld, nasm, objdump, dig, nmap, Wireshark, netstat, nc, traceroute, ping, netfilter, iptables

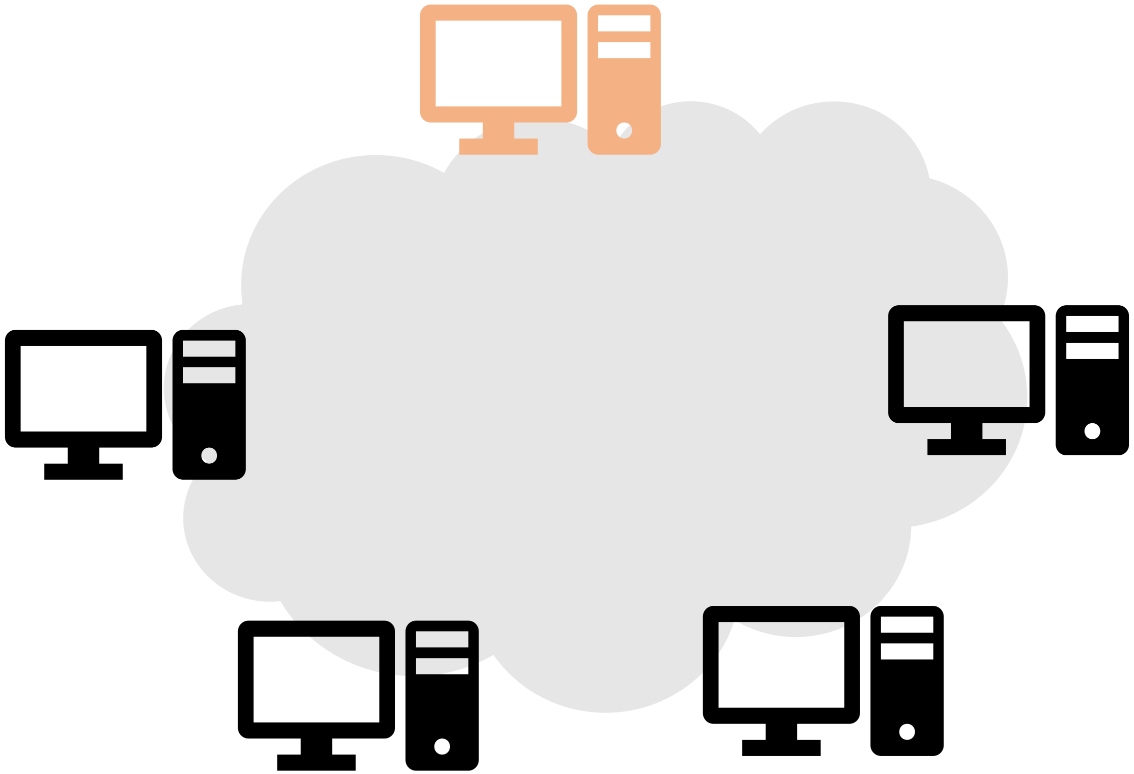
Course Summary

Buffer overflow
Format string vulnerabilities
Frame pointer overwrite
TOCTOU
Integer overflow
Implicit cast
Function reuse attack
Return-to-libc
Return-oriented programming
Shellshock
Dirty COW

StackGuard
Shadow Stack
ASLR
NOEXEC

Course Summary

Port scanning
OS fingerprinting
ARP cache poisoning
TCP SYN flooding
TCP reset attack
TCP session hijacking
TCP seq. number prediction
IP source routing
Local DNS cache poisoning
Remote DNS cache poisoning



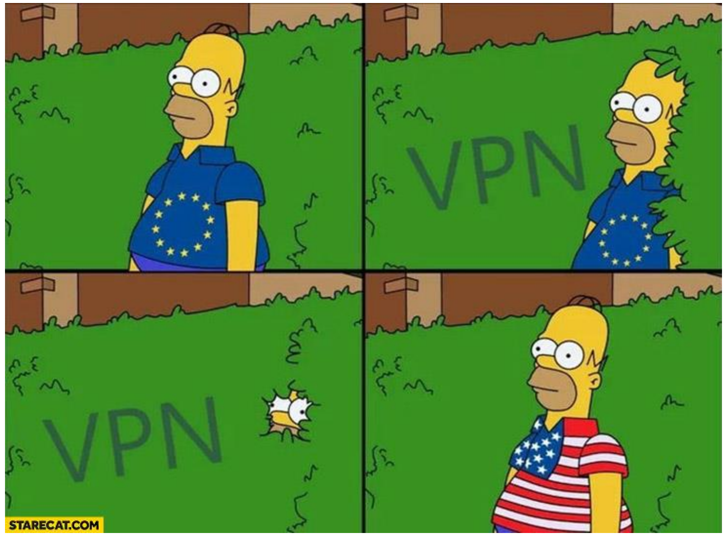
TCP SYN cookie
IPSec
DNSSEC
Firewalls
VPNs

Some Memes

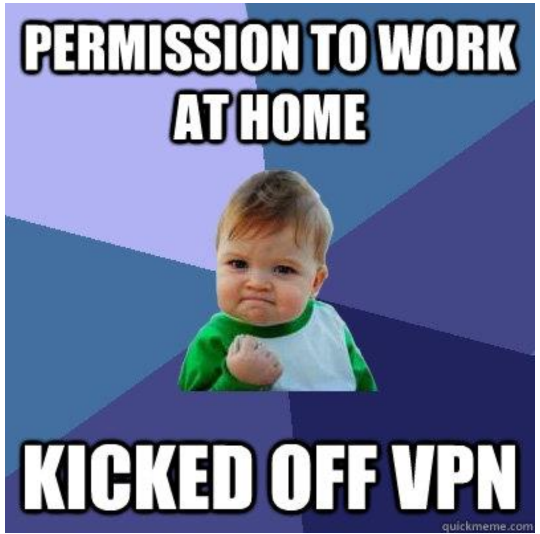
SYN Cookie
Is this a stack canary?

Magic!

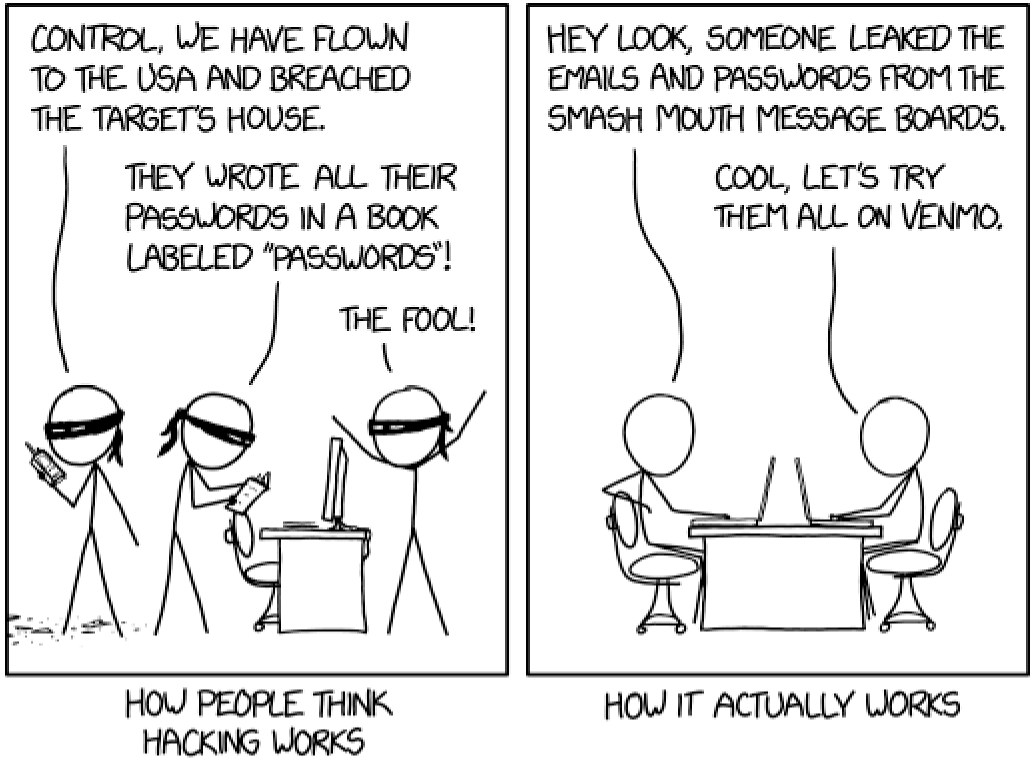
SO YOU’RE TELLING ME, CONTROL DNS
AND I’LL CONTROL MY INTERNET?


VPN
VPN
STARECAT.COM

WITH GREAT POWER COMES
GREAT RESPONSIBILITY
TROLL.ME


PERMISSION TO WORK AT HOME
KICKED OFF VPN
quickmeme.com

Some Comics


CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HOW PEOPLE THINK HACKING WORKS
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW IT ACTUALLY WORKS

"On the Internet, nobody knows you're a dog."

Why Shellcode?

- A private conversation with an industrial collaborator
  - Writing shellcode is a missing skill for most interviewees
- It is essential for many system-related attacks/defenses
- It’s (mostly) fun!

What is Next?

- Not Security-related Career
  - Software engineers
  - System administrator
  - …

Many skills introduced in this course are appreciated/needed in these jobs!

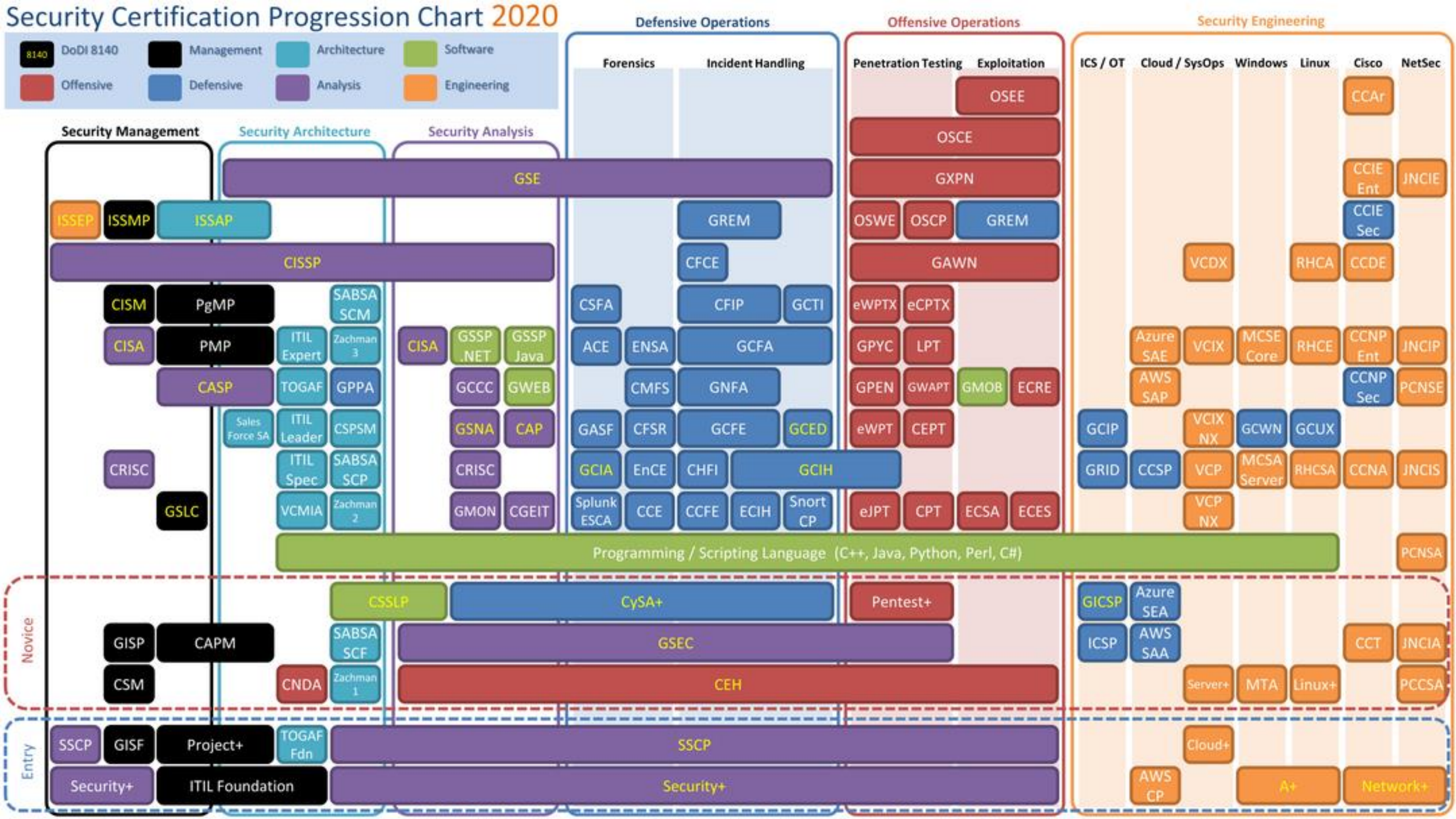
- Security-related Career
  - Red and Blue teams

  - SOC Analyst
  - Ethical Hackers
  - Pen. Testers
  - Security Engineer
  - Network Engineer
  - …

What is Next?

- Penetration Testing
- Risk Management
- Threat Intelligence
- Social Engineering
- …

What is Next? Professional Certifications



Security Certification Progression Chart 2020

8140 DoDI 8140
Management
Architecture
Software
Offensive
Defensive
Analysis
Engineering

Security Management
Security Architecture
Security Analysis
Defensive Operations
Forensics
Incident Handling
Offensive Operations
Penetration Testing
Exploitation
Security Engineering
ICS / OT
Cloud / SysOps
Windows
Linux
Cisco
NetSec

OSEE
CCAr
OSCE
GSE
GXPN
CCIE Ent
JNCIE
ISSEP
ISSMP
ISSAP
GREM
OSWE
OSCP
GREM
CCIE Sec
CISSP
CFCE
GAWN
VCDX
RHCA
CCDE
CISM
PgMP
SABSA SCM
CSFA
CFIP
GCTI
eWPTX
eCPTX
CISA
PMP
ITIL Expert
Zachman 3
CISA
GSSP .NET
GSSP Java
ACE
ENSA
GCFA
GPYC
LPT
Azure SAE
VCIX
MCSE Core
RHCE
CCNP Ent
JNCIP
CASP
TOGAF
GPPA
GCCC
GWEB
CMFS
GNFA
GPEN
GWAPT
GMOB
ECRE
AWS SAP
CCNP Sec
PCNSE
Sales Force SA
ITIL Leader
CSPSM
GSNA
CAP
GASF
CFSR
GCFE
GCED
eWPT
CEPT
GCIP
VCIX NX
GCWN
GCUX
CRISC
ITIL Spec
SABSA SCP
CRISC
GCIA
EnCE
CHFI
GCIH
GRID
CCSP
VCP
MCSA Server
RHCSA
CCNA
JNCIS
GSLC
VCMIA
Zachman 2
GMON
CGEIT
Splunk ESCA
CCE
CCFE
ECIH
Snort CP
eJPT
CPT
ECSA
ECES
VCP NX
Programming / Scripting Language (C++, Java, Python, Perl, C#)
PCNSA

Novice
CSSLP
CySA+
Pentest+
GICSP
Azure SEA
GISP
CAPM
SABSA SCF
GSEC
ICSP
AWS SAA
CCT
JNCIA
CSM
CNDA
Zachman 1
CEH
Server+
MTA
Linux+
PCCSA

Entry
SSCP
GISF
Project+
TOGAF Fdn
SSCP
Cloud+
Security+
ITIL Foundation
Security+
AWS CP
A+
Network+

Example: Offensive Security Certified Professional (OSCP)

- Some skills learned here:
  - Many Linux tools
  - Network protocols
  - Buffer overflow
  - Port scanning
  - OS security
  - Port forwarding
  - Tunneling

Example: GIAC Certified Intrusion Analyst (GCIA)

- Some skills learned here:
  - Many tools
  - Traffic analysis
  - Network protocols
  - Packet filters
  - Wireshark, scapy
  - Monitoring hardware

What is Next? Academic Certifications

- An example:
  - SFU PMP in Cybersecurity
    - Pen testing and ethical hacking
    - Risk management
    - Attacks/defenses on systems and networks
    - Cloud and mobile security
    - Applied cryptography
    - Machine learning for cybersecurity
    - …

To summarize…

- Cybersecurity is a **BIG** and **DiVe*R*sE** field!

- Keep learning (reading and doing)
- Break things (in your VM ☺)
- CTFs
- …