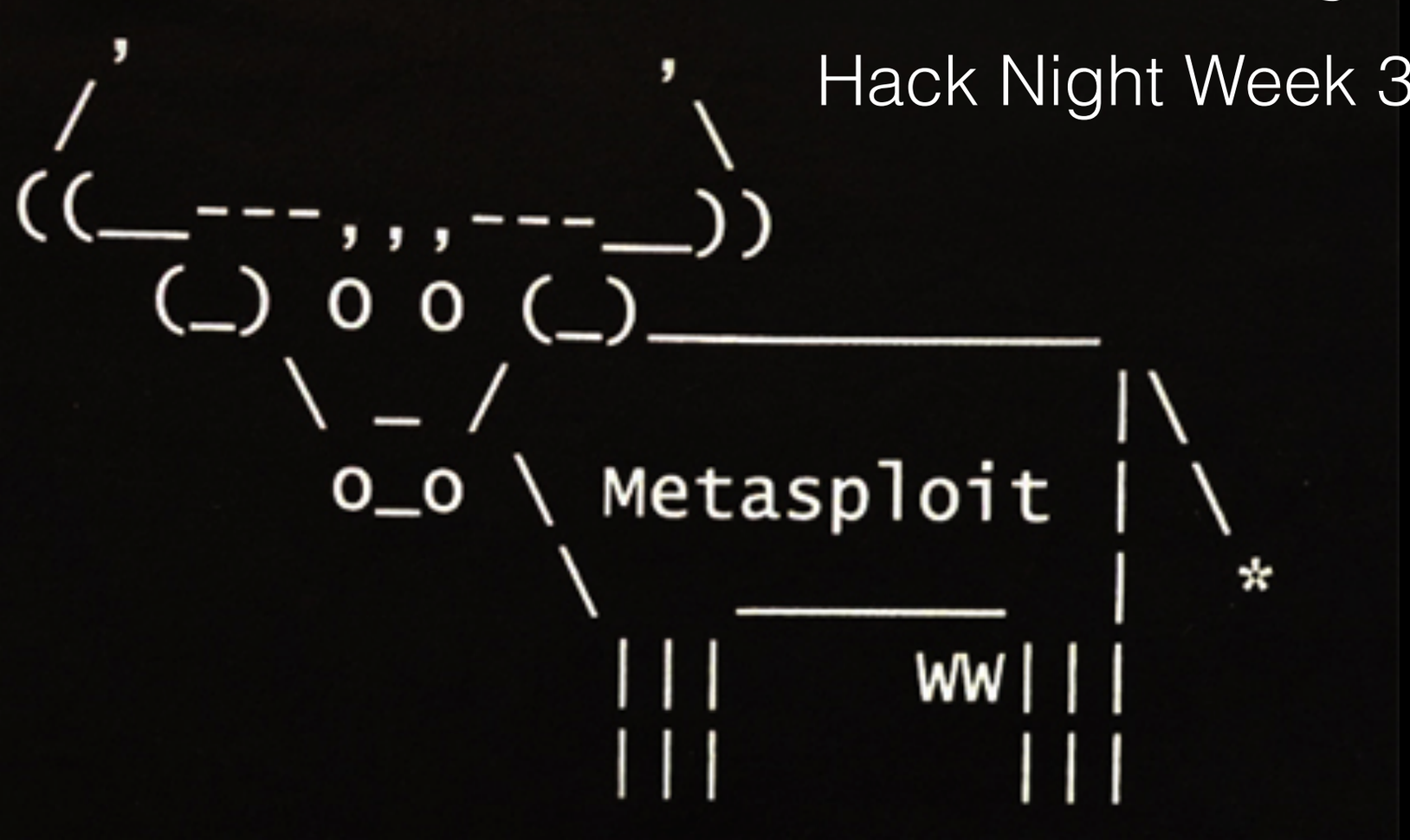
using metasploit to hack everyone

Hack Night Week 3



Vulnerability Disclosure

what you should know

- **computer** - the magical unicorn on your desk
- **program** - anything that runs on your unicorn
- **bug** - a signal line or entire block of code that could cause the program to do something crazy
- **vulnerability** - a bug that might allow a person to take over the program
- **exploit** - some sort of input to the program that exploits a vulnerability to make the program do something it was not intended to do (ie. give a standard user admin privileges)

zero day vulnerabilities

- bugs in code that do not have a fix yet
- zero refers to the number of days since a fix has been made by a developer and released to the wild

hacked team

- on July 5th, Hacking Team, a cyber security firm, had 500 GB of their data leaked online
- among the dump's contents was email corespondance regarding the selling of exploits (big no no)
- Windows + Adobe Flash zero days

]HT[**Hacked Team**
@hackingteam

Follow

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1IhChT!rbB... infotomb.com/eyyxo.torrent

RETWEETS 57 FAVORITES 32

5:26 PM - 5 Jul 2015

Exploit Database

- https://www.exploit-db.com/
- collection of exploits found in the wild
- google dorks
    - using google to find vulnerable websites
- research papers
    - you can find modern exploit techniques here

Seclists Fulldisclosure

- http://seclists.org/fulldisclosure/
- mailing list of any recently disclosed vulnerabilities
- mostly consist of website bugs
- usually link to helpful blog posts

List Archives

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2015	134	101	165	115	133	112	126	86	53	–	–	–
2014	194	273	434	325	213	174	167	89	115	135	103	138
2013	282	162	290	263	227	259	277	303	187	294	222	224
2012	611	477	390	382	323	428	394	393	210	277	236	280
2011	584	687	439	561	572	565	367	393	370	995	466	511
2010	637	502	564	453	408	631	417	445	414	523	342	696
2009	979	380	465	318	282	292	550	455	421	339	386	502
2008	615	496	600	821	681	403	591	559	639	531	739	634
2007	593	629	573	744	555	661	662	530	709	935	582	641
2006	992	740	1865	865	789	1058	770	771	578	678	545	493
2005	939	676	950	666	678	437	766	1078	890	677	1065	1531
2004	1358	1534	1499	1153	1451	1031	1370	1314	1091	1174	1424	731
2003	505	405	296	500	421	892	1251	1942	1763	1806	1123	782
2002	–	–	–	–	–	–	314	835	685	381	456	313

bug bounties

- websites and software companies offer $$$ to those who find flaws in their code
- Pwn2Own
    - people go to show off their browser exploits and make mad money
    - Vupen won $400,000 in 2014

Zero Day Initiative

- http://www.zerodayinitiative.com/
- sell the bugs you find for $$$

people that find bugs

- black hat hackers (people who do bad things with the bugs they find)

- Trail of Bits - https://www.trailofbits.com/ (based in New York)

- bug hunters