



Introductory Proxy and MitM Techniques

By
Rajendra Umadas

Agenda

- Who am I?
 - Rajendra Umadas
- Types of Targets
 - Web App
 - Internal
 - ...
- Man in the Middle Understanding
- Develop custom proxy
 - Recon
 - MITM
 - Edit
 - Own!
- Example

Who Am I

Other than carbon-based multi-cellular life forms



Rajendra Umadas

- Bitten by security bug in NYU:Poly
- Mobile Application Security == fun
 - Legacy Bugs
- Blackhat, OWASP, CMU, NYU:Poly



What we try to break???

Targets

- Web Application Assessments
 - Burp
 - Paros
 - SSL Digger
- Internal
 - Cain and Abel
 - NMAP
 - ...
- So many more

Take Aways

- Tools are important
- Techniques are MORE important
- Understanding is the MOST important
- So I have a question...

Mighty Morphing Network Stream Time!

Setting Up MITM

Checklist

- Set up Linux AP/ Gateway
- Sniff Traffic
- Iptables Magic
- Spin Up Python Proxy

Gateway

- Ubuntu
 - `echo "1" > /proc/sys/net/ipv4/ip_forward`
 - Tell kernel to enable ip forwarding (What a router does)
 - `iptables -t nat -a POSTROUTING -o eth0 -j MASQUERADE`
 - Tell netfilter module to perform Port Address Translation
 - DHCPD: DHCP Server
 - Give out IPs automatically
 - HOSTAPD: (Optional)
 - Make netbook look like AP

Sniff Traffic

- Connect handset to AP
- Start Wireshark
- Sniff
- Capture:
 - Server IP
 - Server Port
 - Quick Recon on possible application transport protocols (HTTP, AMF, ASN1, Proprietary)

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
121	29.119436			UDP	Source port: 58073 Destination port: 46497
158	31.138347			UDP	Source port: 58073 Destination port: 46497
186	35.151134			UDP	Source port: 58073 Destination port: 46497



0050	32 06 d4 6d 7c e7 9d ed	a2 91 19 8c e7 78 b0 81	2..m
0060	cb 84 5f 80 69 a7 4a b9	3c 0b 69 da 02 96 1d 63	.._i.J. <.i....c
0070	98 79 c8 1e aa c1 50 98	05 27 d7 0d 30 2d 9c 4c	.y....P. '..0-.L
0080	0b 0e b6 f8 d1 be 64 df	7d eb 50 62 ab bf 9f 13	d. }.Pb....
0090	79 74 e8 2b ab 05 dd 3e	df	yt.+...> .

Follow UDP Stream

Stream Content

```
00000000 26 18 02 de d4 f0 dd c8 85 6e 26 7e 9c fd 3e ad &..... .n&~..>.
00000010 ec c5 2f 33 23 fc 5f a9 00 63 fc f2 98 7f 2b f7 ../3#.._ .c....+.
00000020 07 dd a6 ba 11 fb 4f 82 b6 f0 84 4f b0 c8 28 3f .....0. ...0..(?)
00000030 c5 9d ad b8 1d 8d 68 4a 31 3d 57 38 6a a6 24 74 .....hJ 1=W8j.$t
00000040 fd 03 55 dd e3 82 8d 20 2c 64 7f b0 f8 21 4a 88 ..U..... ,d...!J.
00000050 26 6f 01 f6 16 c0 8d aa 52 42 fc 3e 9d 55 28 4c &o..... RB.>.U(L
00000060 19 10 db e9 e6 3b 8d 79 e4 62 0d b4 a9 d0 50 .....;y .b....P
00000070 26 18 02 9e a2 47 21 c8 85 6e 26 6b d1 d0 cd 21 &....G!.. .n&k...!
00000080 e6 3b 9b 33 77 fc 36 1b de 27 3a 86 68 5a 38 71 .;.3w.6. .'':hZ8q
00000090 45 be ba a5 93 f7 38 45 42 36 1c 9d 93 95 66 af E.....8E B6....f.
000000A0 02 99 87 73 0b ec da a5 7e e6 28 40 75 3a b6 0f ....s..... ~.(@u:...
000000B0 3d 44 e3 d2 13 83 07 a9 95 d2 47 df b0 9a d3 92 =D..... ..G.....
000000C0 f1 15 d4 bd 6b 18 54 50 f4 92 dd 11 bc 25 0e 75 ....k.TP .....%.u
000000D0 7a 6f ee fa 07 1f f6 df 43 d8 db e7 a7 64 35 zo..... C....d5
000000E0 26 18 02 35 60 08 5f c8 85 6e 26 84 77 41 59 3b &..5'. .. .n&.wAY;
000000F0 63 b5 c3 b6 bb 7d 42 01 d4 9f 4e 66 ec c4 a5 b9 c....}B. ..Nf....
00000100 de 18 20 fb 00 28 32 06 d4 6d 7c e7 9d ed a2 91 .. ..(2. .m|.....
00000110 19 8c ef f8 b0 81 cb 84 5f 80 69 a7 4a b9 3c 0b .....i.J.<.
00000120 69 da 02 96 1d 63 98 79 c8 1e aa c1 50 98 05 27 i....c.y ...i.J.<.
00000130 d7 0d 30 2d 9c 4c 0b 0e b6 f8 d1 be 64 df 7d eb ..0-.L. ....d.}.
00000140 50 62 ab bf 9f 13 79 74 e8 2b ab 05 dd 3e df Pb....yt .+...>.
```

Find Save As Print Entire conversation (333 bytes)

Iptables Magic

- `-A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 1231`
- `-A PREROUTING -i eth1 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 1232`
- `-A PREROUTING -i <lan int> -p tcp -m tcp --dport <remote server port> -j REDIRECT --to-ports <local proxy port>`

Proxy: Python (More Interesting)

- Two Sockets
 - Local Listening Socket (S₁)
 - Socket Connected to Remote Server (S₂)
- S₁ ↔ Manipulation Code ↔ S₂
- <http://code.activestate.com/recipes/483730/>

Example!

I didn't set this up prior... LIVE HACKING...WEAR HARDHAT!

What are we (ME and YOU) doing...

- Short Break
 - Ill set up projector
- After break
 - Lets look at a mobile app...
 - You tell me how to hack it!

The End

■ Questions

